SRC Component Logging

Published: 2014-12-10

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

SRC Component Logging

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- C Series

Documentation Conventions

Table 1 on page viii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Documentation Conventions

Table 1 on page viii defines the notice icons used in this guide. Table 3 on page ix defines text conventions used throughout this documentation.

Table 2: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 3: Text Conventions

Convention	Description	Examples
Bold text like this	• Represents keywords, scripts, and tools in text. • Represents a GUI element that the user selects, clicks, checks, or clears.	• Specify the keyword **exp-msg**. • Run the **install.sh** script. • Use the **pkgadd** tool. • To cancel the configuration, click **Cancel**.
Bold text like this	Represents text that the user must type.	**user@host# set cache-entry-age** *cache-entry-age*

`Fixed-width text like this`	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	`nic-locators {`
		`  login {`
		`  resolution {`
		`  resolver-name /realms/`
		`  login/A1;`
		`  key-type LoginName;`
		`  value-type SaeId;`
		`  }`

Regular sans serif typeface	• Represents configuration statements. • Indicates SRC CLI commands and options in text. • Represents examples in procedures. • Represents URLs.	• **system ldap server{ stand-alone;** • Use the **request sae modify device failover** command with the **force** option • **user@host# . . .** • http://www.juniper.net/techpubs/software/management/sdx/api-index.html

Table 3: Text Conventions *(continued)*

Italic sans serif typeface	Represents variables in SRC CLI commands.	**user@host# set local-address *local-address***
Angle brackets	In text descriptions, indicate optional keywords or variables.	Another runtime variable is <gfwif>.
Key name	Indicates the name of a key on the keyboard.	Press Enter.
Key names linked with a plus sign (+)	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Italic typeface	• Emphasizes words. • Identifies book names. • Identifies distinguished names. • Identifies files, directories, and paths in text but not in command examples.	• There are two levels of access: *user* and *privileged*. • *SRC-PE Getting Started Guide.* • *o=Users, o=UMC* • The */etc/default.properties* file.
Backslash	At the end of a line, indicates that the text wraps to the next line.	Plugin.radiusAcct-1.class=\ net.juniper.smgt.sae.plugin\ RadiusTrackingPluginEvent
Words separated by the | symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic | line

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/cgi-bin/docbugreport/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

Software Features Overview

SRC Component Overview

The SRC software is a dynamic system. It contains many components that you use to build a subscriber management environment. You can use these tools to customize and extend the SRC software for your use and to integrate the SRC software with other systems. The SRC software also provides the operating system and management tools for C Series Controllers.

Table 4 on page 3 gives a brief description of the components that make up the SRC software.

Table 4: Descriptions of SRC Components

Component	Description
Server Components	
Service activation engine (SAE)	• Authorizes, activates, and deactivates subscriber and service sessions by interacting with systems such as Juniper Networks routers, cable modem termination system (CMTS) devices, RADIUS servers, and directories. • Collects accounting information about subscribers and services from routers, and stores the information in RADIUS accounting servers, flat files, and other accounting databases. • Provides plug-ins and application programming interfaces (APIs) for starting and stopping subscriber and service sessions and for integrating with systems that authorize subscriber actions and track resource usage.
Subscriber Information Collector (SIC)	Used in conjunction with the MX Series router running the packet-triggered subscribers and policy control (PTSP) solution, the SIC listens for RADIUS accounting events from IP edge devices (accounting clients) and stores them in the Session State Registrar (SSR), or forwards them to a remote AAA server, allowing the SRC software to gain increased subscriber awareness. Additionally, the SIC can optionally edit accounting events before routing them.
Juniper Policy Server (JPS)	Acts as a policy decision point (PDP) and policy enforcement point (PEP) that manages the relationships between application managers and CMTS devices in a PCMM environment.
Network information collector (NIC)	Collects information about the state of the network and can provide a mapping from a given type of network data to another type of network data.

Table 4: Descriptions of SRC Components *(continued)*

Component	Description
Redirect Server	Redirects HTTP requests received from IP Filter to a captive portal page.
3GPP Gateway	The SRC Third-Generation Partnership Project (3GPP) gateway is a Diameter-based component in the SRC software, which provides integration with 3GPP Policy and Charging Control environments, to provide fixed-mobile convergence (FMC). The SRC 3GPP gateway provides Gx-based integration with the Policy and Charging Rules Function (PCRF). The SRC 3GPP gateway uses the Gx interface to mediate between the PCRF and Juniper Networks routers like the E Series Broadband Services routers and MX Series routers. The Gx interface on the SRC 3GPP gateway communicates with the PCRF using the Diameter protocol.
Web Application Service	The SRC software includes a Web application server that hosts the Web Services Gateway and the Volume Tracking Application (SRC VTA). In production environments, this application server is designed to host only these applications. However, you can load your own applications into this server for testing or demonstration purposes.
Web Services Gateway	Allows a gateway client—an application that is not part of the SRC network—to interact with SRC components through a Simple Object Access Protocol (SOAP) interface. The Web Services Gateway provides the Dynamic Service Activator which allows a gateway client to dynamically activate and deactivate SRC services for subscribers and to run scripts that manage the SAE.
Repository	
Directory	The SRC software includes the Juniper Networks database, which is a built-in Lightweight Directory Access Protocol (LDAP) directory for storing all SRC data including services, policies, and small subscriber databases. For large subscriber databases, you must supply your own directory.
Session State Registrar (SSR)	The SSR is a stateless, highly reliable and highly available database cluster. When used in conjunction with an MX Series router running the packet-triggered subscribers and policy control (PTSP) solution, the SSR stores the IP edge attachment subscriber sessions data learned from IP edge devices in the centralized SSR database.
SRC Configuration and Management Tools	
SRC command line interface (CLI)	Provides a way to configure the SRC software on a C Series Controller from a Junos OS–like CLI. The SRC CLI includes the policies, services, and subscribers CLI, which has separate access privileges.
C-Web interface	Provides a way to configure, monitor, and manage the SRC software on a C Series Controller through a Web browser. The C-Web interface includes a policies, services, and subscribers component, which has separate access privileges.
Simple Network Management Protocol (SNMP) agent	Monitors system performance and availability. It runs on all the SRC hosts and makes management information available through SNMP tables and sends notifications by means of SNMP traps.
Service Management Applications (Run on external system)	

Table 4: Descriptions of SRC Components *(continued)*

Component	Description
IMS Services Gateway	Integrates into an IP multimedia system (IMS) environment. The SRC software provides a Diameter protocol-based interface that allows the SRC software to integrate with services found on the application layer of IMS.
SRC Programming Interfaces	
NETCONF API	Allows you to configure or request information from the NETCONF server on a C Series Controller that runs the SRC software. Applications developed with the NETCONF API run on a system other than a C Series Controller.
CORBA plug-in service provider interface (SPI)	Tracks sessions and enables linking the rest of the service provider's operations support system (OSS) with the SRC software so that the OSS can be notified of events in the life cycle of SAE sessions. Hosted plug-ins only.
CORBA remote API	Provides remote access to the SAE core API. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
NIC access API	Performs NIC resolutions. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
SAE core API	Controls the behavior of the SRC software. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
Script services	Provides an interface to call scripts that supply custom services such as provisioning policies on a number of systems across a network.
VTA API	The Volume Tracking Application (VTA) API is a Simple Object Access Protocol (SOAP) interface that allows developers to create gateway clients and that administrators use to manage VTA subscribers and sessions. The SRC Web Services Gateway allows a gateway client—an application that is not part of the SRC network—to interact with SRC components, such as the VTA, through a SOAP interface.
Authorization and Accounting Applications	
AAA RADIUS servers	Authenticates subscribers and authorizes their access to the requested system or service. Accepts accounting data—time active and volume of data sent—about subscriber and service sessions. RADIUS servers run on a system other than a C Series Controller.
SRC Admission Control Plug-In (SRC ACP)	Authorizes and tracks subscribers' use of network resources associated with services that the SRC application manages.
Flat file accounting	Stores tracking data to accounting flat files that can be made available to external systems that send the data to a rating and billing system.

Table 4: Descriptions of SRC Components *(continued)*

Component	Description
Volume Tracking Application	The SRC Volume Tracking Application (SRC VTA) is an SRC component that allows service providers to track and control the network usage of subscribers and services. You can control volume and time usage on a per-subscriber or per-service basis. This level of control means that service providers can offer tiered services that use volume as a metric, while also controlling abusive subscribers and applications. When a subscriber or service exceeds bandwidth limits (or quotas), the SRC VTA can take actions including imposing rate limits on traffic, sending an e-mail notification, or charging extra for additional bandwidth consumed.
Demonstration Applications (available on the Juniper Networks Web site)	
Enterprise Audit Plug-In	Defines a callback interface, which receives events when IT managers complete specified operations.
Enterprise Manager Portal	Allows service providers to provision services for enterprise subscribers on routers running JunosE or Junos OS and allows IT managers to manage services. Enterprise Manager Portal can be used with NAT Address Management Portal to allow service providers to manage public IP addresses for use with NAT services on routers running Junos OS and to all IT managers to make requests about public IP addresses through the Enterprise Manager Portal.
Monitoring Agent application	Integrates IP address managers, such as a DHCP server or a RADIUS server, into an SRC-managed network so that the SAE is notified about subscriber events. The Monitoring Agent application runs on a Solaris platform.
Residential service selection portals	Provides a framework for building Web applications that allow residential and enterprise subscribers to manage their own network services. It comes with several full-featured sample Web applications that are easy to customize and suitable for deployment. The Residential service selection portals run on a Solaris platform.
Sample enterprise service portal	Lets service providers supply an interface to their business customers for managing and provisioning services.

Related Documentation

- *SRC Product Description*

CHAPTER 2

Logging for SRC Components

Logging for SRC Components Overview

SRC components and applications generate event messages that you can save in logs—either by writing the messages to text files or by using the system log facilities. You can use these logs to monitor the SRC components and troubleshoot problems.

Each SRC component has its own logging configuration. For example, the license server, the NIC, the SAE, and SNMP each have logging configuration. The C Series Controller includes a system log server that you can configure to manage messages generated on that platform. You can use the CLI and the C-Web interface to configure logging on a C Series Controller and to configure the system log server on a C Series Controller.

When you enable logging to a file, by default SRC components and applications write log files to the **/opt/UMC/<component-directory>/var/log** folder for a component, such as **/opt/UMC/sae/var/log**.

All log files with the file extension .log in a *var/log* directory are "Rotating Log Files" on page 22.

Related Documentation

- *C Series Controller Log Server Overview*
- The system log Protocol—draft-ietf-syslog-protocol-16.txt (July 2006 expiration)
- *Configuring the SRC SNMP Agent (SRC CLI)*
- Configuration Statements for SRC Component Logging on page 41
- Categories and Severity Levels for Event Messages on page 7

Categories and Severity Levels for Event Messages

In the logging configuration, you can specify a filter for each type of log. This filter can include an expression that defines the *categories* and *severity levels* of event messages

that the software saves. You can also enable network device-specific filtering for service activation engine (SAE) debug logs.

Defining Categories

The category of an event message defines the SRC component that generated the event message. If you want to view only event logs in a specific category, you can define a variable <category>, which is a text string that matches the name of a category. This variable is not case sensitive. To view the names of categories for event messages, view a log file for one of the default filters.

For example purposes, Table 5 on page 8 lists the SAE logging categories and associated severity levels. These categories are relevant only for loggers configured with the **shared sae .... configuration logger** statement. The extension refers to loggers that dynamically change their name at runtime. Juniper Networks Customer Service can also provide names of categories for other components, especially for troubleshooting purposes.

Table 5: SAE Categories and Severity Levels

Category	Extension	Severity Level
AAAExtIntf		error, debug, debug_8
AAAExtIntfIDGenerator		error
AAALdapListener		error, debug
AAARouterDriver		info, error, debug
AAASolicitedJob		info, warning, error, debug
AccessManager		info, error, debug
AccountingFileDict		info, error, debug
AccountingFilePeer		info, error, debug
ACPIntfListener		error, debug
ACRMsg		warning, debug
AddressCtx		info, error, debug
Admin		info, error, debug
AggregateServiceSession		error, debug
AMGroupLDAPListener		info, debug
ASRMsg		warning, debug
Atom		debug

Table 5: SAE Categories and Severity Levels *(continued)*

Category	Extension	Severity Level
BEEPDebug	-	debug_9
ClassifyDhcp		error, debug
ClassifyInterface		info, error, debug
ClassifyUser		error
Client	/	info, error, debug
ClientMgr	/	info, error, debug
Commands		error
CommunityManager		error, debug
CommunityMember		info, error, debug, debug_9
ConfigChecker		info, error, debug
COPSDecoder		info, debug_9
COPSEncoder		info, debug_10
Core API		error, debug
CustomRadiusAccounting		error, debug
CustomRadiusAuth		error, debug
DataManagerMIData		error
DCImpl		warning, error, debug
DhcpManager		error, debug
DhcpOptions		error
DiameterDriverManager		info, error, debug
DiameterMsgHandler		warning, error, debug, debug_8
DiameterPlacementProcessor		error
DiameterRouterDriver		info, warning, error, debug
DiameterUnsolictedMsg		info, warning, error, debug

Table 5: SAE Categories and Severity Levels *(continued)*

Category	Extension	Severity Level
DiscoverDecisionHelper		error
DynRadiusServer		error, debug
EmbeddedPrecedenceProcessor		error, debug_9
EquipRamCache		debug
EquipRegLdapDataManager		info, error, debug
EquipRegLDAPDataManagerConnectionThread		info, error, debug
EventBatch		error, debug
EventPublisher		error, debug
Extension Script		info, error, debug
ExtInterface		info, warning, error, debug
ExtIntf		info, error, debug
FailQueue		error, debug
FeedbackManager		info, error
FileDeleter		info, error, debug
FileRotater		info, error, debug
FileTrackingPluginEventListener		info, error, debug
FlexibleRadiusAuthPluginEventListener		info, error, debug
FlexibleRadiusTrackingPluginEventListener		info, error, debug
FloatingContext		info, error, debug
GateProcessor		error, debug
GenericService		error, debug
GenericSessionJobManager		info, error, debug
HostUtil		error, debug
HttpAttachmentProcessor		info, error, debug

Table 5: SAE Categories and Severity Levels *(continued)*

Category	Extension	Severity Level
IdleTimeoutObject		debug
InfrastructureServiceSession		error, debug
InterfaceSession		error
InterfaceTimeoutManager		debug
InterimSessionJobManager		info, error, debug
IpInterfaceCtx		info, error, debug
ISEExtIntf		error, debug
ISEPORetriever		error, debug
ISEProvisioningContext		error
ISERouterDriver		info, warning, error, debug
ISESolicitedJob		info, warning, error, debug
JobQueue		info, debug_9
JunoScriptConfHelper	-	info
JunoScriptSubChannelHandler	-	debug, trace
JunosDriverManager		info, error, debug
JunosEDriverManager		info, error, debug
JunosEIcc		error, debug
JunoseJob		error, debug
JunosERouterDriver		info, error, debug, debug_9, perf
JunosERouterFactory		info
JunosEXDRRouterDriver		info, error, debug, debug_9, perf
JunosRouterDriver		info, error, debug, debug_9
JunosRouterFactory		info
JunosServiceActivationPoint		error, debug

Table 5: SAE Categories and Severity Levels *(continued)*

Category	Extension	Severity Level
JunosSessionManager		error, debug
JunosSyslogConfigHandler		info, error, debug
JunosSyslogSubChannelHandler		info, error, debug
KeepAliveTimer		error
LdapAuthenticator		error, debug
LDAPConfManager		error
LicenseCheck		info, error
LicenseLDAPListener		debug
LicenseManager		info, error, debug
LicenseServerClient		info, error, debug
LicenseUtil		debug
LimitNumSubscriberPerIntfAuthPluginListener		debug
ListenerJobManager		debug
LiveSessions	/	info, error, debug
LocalPersistentCheck		error
LoginNameParser		error
LoginRequest		error, debug
LogoutRequest		error, debug
Main		info, debug, panic
MemFailQueue		error, debug
MsgInOps		info, error, debug_8
MsgOutPostUpdateOps		info, debug, debug_8
MsgOutUpdateOps		info, debug
NasPortUtil		debug

Table 5: SAE Categories and Severity Levels *(continued)*

Category	Extension	Severity Level
NicProxyCompleter		error
OpsBuffer		info, error, debug
PingJob		error, debug_9
PluginManager		info, error, debug
PluginUtil		error
PolicyParameterEngine		debug_8
PolicyDecisionPointLDAPListener		info, debug
PolicyListAugmentingProcessor		info, error, debug
PolicyLists		debug_9
PolicyListSharingProcessor		error, debug
PolicyPPRMsg		warning, error, debug
PolicyServiceSession		error, debug
PolicySharedCtx		info, error, debug
Portal API		error, debug
PostponedScheduledService		debug
PostSyncJob		debug
ProcessorManager		error, debug
ProxyDriverManager		error, debug
ProxyRouterDriver		info, error, debug, debug_9
ProxySessionManager		info, error, panic
PTSPRouterDriver		error, debug
PublisherQueue		info, error, debug
QoSAttachmentProcessor		info, error, debug
QosProfileTrackingEntry		info, error, debug

Table 5: SAE Categories and Severity Levels *(continued)*

Category	Extension	Severity Level
QTPEventListener		info, error, debug
QTPJobQueue		error
QTPThreadPoolThread		error, debug
RadiusAuthPluginEventListener		info, error, debug
RadiusPacket		error, debug
RadiusPeer	-	info, error, debug, debug_9
RadiusPeerGroup	-	info, error, debug
RadiusPluginEventListener		info, error, debug
RadiusSocket		info, error, debug, debug_9
RadiusTrackingPluginEventListener		info, error, debug
ReadyToSyncJob		error, debug_9
RefCounter		error
ReferencedPrecedenceProcessor		error, debug_9
ReferencedProcessor		error, debug
RemotePlugin		info, error, debug
ReplayJob		error, debug
Replicator		info, error, debug, debug_9
Retailer		error, debug
RetailerLdapListener		error, debug
RksEventListener		info, error, debug
RksPluginPublisher		error, debug
RouteConfigPPRMsg		warning, error, debug
RouterComponent		info, error
RouterLDAPListener		debug

Table 5: SAE Categories and Severity Levels *(continued)*

Category	Extension	Severity Level
RouterRegistry		info, error, debug
RouterScript		info, error, debug
RouterScriptComponent		error
SAEAccessImpl		debug
SAE-AUDIT		info, notice, warning
SchedulingAuthPlugin		info, error, debug
ScriptServiceSession		info, error, debug
ServiceActivator		info, error, debug
ServiceAuthEvent		debug
ServiceFragment		debug
ServiceLDAPDataManager		info, error, debug
ServiceLDAPDataManagerConnectionThread		info, error, debug
ServiceLdapListener		error, debug
ServiceManager		error, debug
ServiceMutexGroup		error
ServiceMutexGroupLdapListener		info, error, debug
ServiceMutexGroupManager		debug
ServiceProfile		error
ServiceProfileLdapListener		error, debug
ServiceSchedule		error
ServiceScheduleLdapListener		info, error, debug
ServiceScheduleManager		debug
ServiceScopeLdapListener		info, error, debug
ServiceSession		info, error, debug

Table 5: SAE Categories and Severity Levels *(continued)*

Category	Extension	Severity Level
ServiceSessionAttributes		debug
ServiceVrLdapListener		info, error, debug
SessionAudit		notice
SessionFactory		info, error, debug
SessionJob		error
SessionJobManager		info, error, debug
SessionStoreFactory		info, error, debug
SessionStoreImpl	/	info, error, debug
SimRouter		info, warning, error, debug
SimRouterDriver		info, error, debug, debug_9
Slave	/	info, error, debug
SlaveMgr		info, error, debug
SolicitedReplyFactory		error, debug, debug_9
SRQMsg		warning, debug
SSFile		info, error, debug
SSFiles	/	info, error, debug, debug_6
SspAccRadiusPeerMI		info, error
SspAuthRadiusPeerMI		info, error
SspSM		info, error, debug
SsrAttributePluginHelper		error, debug
SsrEventHandler		info, error, debug
SSREventJob		error
SsrReaderPluginEventListener		error, debug
SSRServiceEventJob		info, error, debug

Table 5: SAE Categories and Severity Levels *(continued)*

Category	Extension	Severity Level
SSRSubscriberEventJob		info, error, debug
SsrWriterPluginEventListener		info, error, debug
StateSynchronizer		info, error, debug
Stats		info, error, debug
StoreConfig		info, error, debug
StoreOpIterator		debug, debug_8
SubscriberRef		info, error, debug
SubscriberScheduleLdapListener		error, debug
SubscriberScheduleManager		debug
SubscriptionParser		error
Table		debug
TestMaster		info, error, debug
TestPromo		debug
TimeoutSessionJobManager		info, error, debug
TimePolicyManager		info, error, debug
Transaction		error, debug, debug_9
TransactionManager		debug, debug_9
UCCImpl		error, debug
UnsolicitedMessage		error, debug
UnsolicitedMsgFactory		debug
UnsolicitedTimeoutJob		error, debug
UserLDAPDataManager		info, error, debug
UserLDAPDataManagerConnectionThread		info, error, debug
UserLdapListener		debug

Table 5: SAE Categories and Severity Levels *(continued)*

Category	Extension	Severity Level
UserManager		error, debug
UserProfile		error, debug
UserProfileManager		debug
UserRamCache		debug
UserSession		info, error, debug
WrapperServiceSession		error, debug

Defining Severity Levels

The event filter provides 128 levels of severity numbered 1–127. A higher number indicates a higher level of severity. Common levels of severity also have a specific name, as shown in Table 6 on page 18.

CAUTION: Enabling the generation of debug log messages has a negative affect on system performance. Do not enable debug log messages unless you are instructed to do so by Juniper Networks Technical Assistance Center (JTAC).

Table 6: Named Severity Levels

Name	Severity Level
logmin	1
debug	10
info	20
notice	30
warning	40
error	50
crit	60
alert	70
emerg	80
panic	90

Table 6: Named Severity Levels *(continued)*

Name	Severity Level
logmax	127

You can define a severity level as follows:

- Specify an explicit severity. For example:
  - debug—Defines only debug messages
- Specify a minimum severity and a maximum severity. For example:
  - info-warning—Defines messages of minimum severity level of info and a maximum severity level of warning
  - Accept the default minimum (logmin) or maximum (logmax) severity by omitting the minimum or maximum severity. For example:
  - info-—Defines messages of minimum severity level info and maximum severity level logmax
  - -warning—Defines messages of minimum severity level logmin and maximum severity level warning
- Specify no severities to log all event messages.

The syntax for the severity takes the format:

[<severity>] | [<minimumSeverity>]-[<maximumSeverity>]

Use either the name or the number of a severity level shown in Table 6 on page 18 for the variables in this syntax.

Defining Filters

You specify a filter by defining an expression with the following format:

singlematch [,singlematch]*

- singlematch—[!] (<category> | ([<category>]/[<severity>] | [<minimumSeverity>]-[<maximumSeverity>]))
- !—Do not log matching events
- <category>—See "Defining Categories" on page 8
- [<severity>] | [<minimumSeverity>]-[<maximumSeverity>]—See "Defining Severity Levels" on page 18.

The software filters events by evaluating each subexpression in order from left to right. When the software determines that an event message matches a subexpression, the software logs or ignores the message accordingly. You can specify an unlimited number of subexpressions; however, the order in which you specify the subexpressions affects the result.

NOTE: When you configure a filter, you must set appropriate values for categories and severity levels. Otherwise, the commit is not successful and when you commit the changes, a message indicating that the configured filter is invalid is displayed.

Table 7 on page 20 shows some examples of filters.

Table 7: Examples of Filters for Event Messages

Syntax	Event Messages Saved
/	All event messages
/info-	Event messages of level info and above from all categories
Cops/debug	Debug events from COPS category only
!Cops,/debug	All debug events except those from COPS category
CopsMsg/info-,!CopsMsg,Cops	All messages from COPS category, except those from CopsMsg category with level less than info

Enabling Network Device-Specific Filtering for SAE Debug Logs (SRC CLI)

You can enable network device-specific filtering for SAE debug logs based on router name, interface name, or login name by including the **device-filter-key** option under the **shared sae .... configuration logger** hierarchy level. Enabling network device-specific SAE debug log filtering reduces the size of the debug log files, thereby simplifying troubleshooting and minimizing the impact on SAE performance.

You can enable network device-specific filtering of SAE debug logs only if you set the SAE severity level to **debug** and then include the **device-filter-key** option under the **shared sae .... configuration logger** hierarchy level. If you do not set the SAE severity level to **debug**, but enable network device-specific filtering, then no information is logged in to the SAE debug log file. When using network device-specific filtering, you can add one or more device filters by using an expression that defines certain criteria. Only log events matching the criteria are logged in the SAE debug log file. Events that do not match the criteria are not logged in the SAE debug log file.

NOTE: SRC network device–specific filtering for SAE debug logs is supported on JunosE (COPS) and Junos OS (JSRC) devices.

If the network device-specific debug log filtering is not enabled, the SAE debug logger displays its default behavior. By default, log events that match the subexpression defined by using the **filter** option are logged.

You can configure network device-specific debug log filtering by defining an expression with the following format:

deviceFilter [deviceFilter]*

- deviceFilter—OpenQuotes deviceFilterKey CloseQuotes
- deviceFilterKey—SingleDevKey *[Operands SingleDevKey]
- SingleDevKey—varName Equality valName
- varName—“router-name” or “interface-name” or “login-name”
- AlphaNumeric—%x41-5A / %x61-7A / %x30-39 / %x2A
- valName—1*AlphaNumeric
- Equality—“=” or “!=”
- Operands—“&” or “|”
- OpenQuotes—“
- CloseQuotes—”

The deviceFilterKey expression is composed of one or more SingleDevKey expressions. A SingleDevKey expression should begin with an open brace and end with a close brace.

The SAE filters events by evaluating each **deviceFilter** in order from left to right. You can specify an unlimited number of device filters; however, the order in which you specify the device filter affects the result. The SAE only logs event messages that match all the criteria.

NOTE: **After you configure the device-filter-key option, restart the SAE for the configuration to take effect.**

You specify the **deviceFilter** with the format rules described in Table 8 on page 21.

Table 8: SAE Debug Device Filter Formatting Rules

Rule	Definition	Meaning
OpenQuotes	“	Denotes an open single or double quotation mark, which is used at the beginning of an expression
CloseQuotes	”	Denotes a close single or double quotation mark, which is used at the end of an expression
Equality	=	Allows logging of only the *logevent* whose value is equal to the value specified in the *valName*
	!=	Allows logging of only the *logevent* whose value is not equal to the value specified in the *valName*

Table 8: SAE Debug Device Filter Formatting Rules *(continued)*

Rule	Definition	Meaning
Operands	&	Allows logging of only the *logevent* whose value matches the *valName* value specified in all *SingleDevKey* expressions in a *deviceFilterKey*
	|	Allows logging of the *logevent* even if its value matches the *valName* value specified in any one of the *SingleDevKey* expressions in a *deviceFilterKey*
varName	*router-name* or *interface-name* or *login-name*	Variable names supported to specify the **deviceFilterKey**.
valName	*AlphaNumeric*	Value name associated with each variable name. A *valName* can contain alphanumeric characters as well as a wildcard character (*).
SingleDevKey	*varName Equality valName*	Pair of *varName* and *valName* associated by using an *Equality*. Multiple *SingleDevKey* expressions are associated by using *Operands*.

Table 9 on page 22 lists some examples of network device-specific SAE debug filter configurations.

Table 9: Sample Combinations of Conditions for the device-filter-key Expression

Syntax	Notes
set device-filter-key ***"router-name=erx440 & interface-name=Fast*"***	Uses the **AND** operator
set device-filter-key ***"router-name=erx440 | interface-name=Fast*"***	Uses the **OR** operator
set device-filter-key ***"router-name=erx440 & interface-name=Fast* | login-name = jane@virneo.net"***	Uses the **AND** and **OR** operators
set device-filter-key ***"router-name=erx440 & interface-name=Fast* & login-name = jane*net"***	Uses the wildcard character (*) for pattern match
set device-filter-key ***"router-name=erx440 | router-name =erx448"***	Uses multiple **deviceFilterKey** configurations
set device-filter-key ***"router-name=erx440 & interface-name!=Fast*"***	Uses the "not equal to" condition

Related Documentation

- Logging for SRC Components Overview on page 7
- *SNMP Traps Overview*
- Configuring an SRC Component to Store Log Messages in a File (SRC CLI) on page 27

Rotating Log Files

Logrotate is a log file management utility that allows you to manage the large number of log files the SRC software generates. Logrotate is essential for managing the disk space on the C Series Controller.

The following SRC components support the logrotate utility:

- Third-Generation Partnership Project (3GPP) gateway
- SRC Admission Control Plug-in (ACP)
- Activity Monitor
- SNMP agent
- Web application server
- Command-line interface (CLI)
- Diameter server
- Dynamic Service Activator
- IP Multimedia Subsystem (IMS)
- Juniper Policy Server (JPS)
- License server
- Monitoring Agent application
- Network information collector (NIC)
- Service activation engine (SAE)
- Subscriber information collector (SIC)
- Session State Registrar (SSR)
- C-Web interface

You can use logrotate to regularly rotate log files by removing the oldest log files from your system and creating new log files. You can rotate files based on size. You can rotate log files daily, weekly, or monthly. Logrotate can also be used to compress log files. Logrotate usually runs automatically through the Cron utility.

When a new log file is opened to replace an older log file that contains content, a number is appended to the name of the older file. For example, *sae_debug.log.4* is an older log file than *sae_debug.log.1*; *whereas sae_debug.log* is the active log file for SAE.

On C Series Controllers, the software compresses log files and appends the *.gz* suffix; for example, *sae_debug.log.4.gz*. Log files are stored in the */opt/UMC/component-name/var/log directory*; for example, */opt/UMC/sae/var/log*.

You can configure components to send log messages to the system log server on the platform on which the SRC software is running.

If you plan to filter log messages, you should be familiar with severity levels and filters for logging before you configure system logging for a component.

Configuration Overview

You can specify any number of log rotation configuration files on the command line. Configuration options that you specify for a group of log files are considered local options and they override global options of the same name.

Both global and local options can be set in the **/etc/logrotate.conf** file. You set global options under the **[edit system logrotate logrotate.conf]** hierarchy level. You set local options for specific logging configuration files such as the **/var/log/wtmp** file under the **[edit system logrotate logrotate.conf logfiles *name*]** hierarchy level. You can also configure log rotation for system and SRC components under the **[edit system logrotate *file-name* logfiles]** hierarchy level.

Related Documentation

- Logging for SRC Components Overview on page 7
- Configuring an SRC Component to Store Log Messages in a File (SRC CLI) on page 27
- Configuration Statements for the Logrotate Utility (SRC CLI) on page 42
- Configuring the Logrotate Utility (SRC CLI) on page 32

PART 2

Configuration

CHAPTER 3

Configuration Tasks for Logging for SRC Components

Before You Configure Logging for SRC Components

Before you configure logging for SRC components, you should be familiar with the logging filters that you can configure. If you use a system logging facility, you should be familiar with the system log protocol. For information about logging filters see "Logging for SRC Components Overview" on page 7.

If you plan to filter log messages, you should be familiar with severity levels and filters for logging before you configure system logging for a component. See "Categories and Severity Levels for Event Messages" on page 7.

Related Documentation

- Configuring System Logging (SRC CLI) on page 30
- Configuring an SRC Component to Store Log Messages in a File (SRC CLI) on page 27
- Configuration Statements for SRC Component Logging on page 41

Configuring an SRC Component to Store Log Messages in a File (SRC CLI)

Use the following statements to configure an SRC component to store log messages in a file:

```
logger name file {
```

```
    device-filter-key device-filter-key;
    filter filter;
    filename filename;
    rollover-filename rollover-filename;
    maximum-file-size maximum-file-size;
}
```

If you plan to filter log messages, you should be familiar with severity levels and filters for logging before you configure system logging for a component. See "Categories and Severity Levels for Event Messages" on page 7.

To configure component logging to a file:

1. From configuration mode, access the configuration statement that configures the logging destination for the component.

   ```
   [edit]
   user@host# component-hierarchy logger name file
   ```

   For example:

   ```
   [edit]
   user@host# edit shared sae configuration logger sae-file-log-1 file
   ```

   ```
   [edit]
   user@host# edit snmp agent logger snmp-file-log-1 file
   ```

   ```
   [edit]
   user@host# edit slot 0 jps logger jps-file-log-1 file
   ```

2. Specify the filter to define which event messages the software logs or disregards.

   ```
   [edit shared sae configuration logger sae-file-log-1 file]
   user@host# set filter filter
   ```

   If you do not specify a filter, logging to the specified file is disabled.

   Filters can specify the logging level, such as debug, or can specify expressions.

   NOTE: When you configure a filter, you must set appropriate values for categories and severity levels. Otherwise, the commit is not successful and when you commit the changes, a message indicating that the configured filter is invalid is displayed.

3. (Optional) Enable network device-specific filtering for SAE debug logs based on router name, interface name, or login name.

   For more information about format rules used to define the expression while enabling network device-specific filtering, see the table ***SAE Debug Device Filter Formatting Rules*** in "Categories and Severity Levels for Event Messages" on page 7.

   ```
   [edit shared sae configuration logger sae-file-log-1 file]
   user@host# set device-filter-key device-filter-key
   ```

NOTE:

- SRC network device–specific filtering for SAE debug logs is supported on JunosE (COPS) and Junos OS (JSRC) devices.
- The **device-filter-key** option is available only on the SAE component.
- You can enable network device-specific filtering of SAE debug logs only if you set the SAE severity level to **debug** and then include the **device-filter-key** option under the **shared sae .... configuration logger** hierarchy level.
- After you configure the **device-filter-key** option, restart the SAE for the configuration to take effect.

4. Specify the absolute path of the filename that contains the current log files.

   ```
   [edit shared sae configuration logger sae-file-log-1 file]
   user@host# set filename filename
   ```

   Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

5. (Optional) Specify the absolute path of the filename that contains the log history.

   ```
   [edit shared sae configuration logger sae-file-log-1 file]
   user@host# set rollover-filename rollover-filename
   ```

   When the log file reaches the maximum size, the software closes the log file and renames it. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.

   NOTE: On a C Series Controller, log files are rotated according to the settings in the logrotate utility. The logrotate utility specifies how often log files are rotated and whether they are compressed.

6. (Optional) Specify the maximum size of the log file and the rollover file.

   ```
   [edit shared sae configuration logger sae-file-log-1 file]
   user@host# set maximum-file-size maximum-file-size
   ```

   NOTE: The maximum file size is specified in KB. Maximum size of the log file is 10,000,000 KB.

   Do not set the maximum file size to a value greater than the available disk space.

Related Documentation

- Configuring System Logging (SRC CLI) on page 30
- *Saving System Log Messages to a File (SRC CLI)*
- *Sending System Log Messages to Other Servers (SRC CLI)*
- Before You Configure Logging for SRC Components on page 27
- Logging for SRC Components Overview on page 7

Configuring System Logging (SRC CLI)

Use the following statements to configure the SRC software to send log messages to the system logging facility:

```
logger name syslog {
    filter filter;
    host host;
    facility facility;
    format format;
    port port;
}
```

You can configure components to send log messages to the system log server on the platform on which the SRC software is running.

If you plan to filter log messages, you should be familiar with severity levels and filters for logging before you configure system logging for a component. See "Categories and Severity Levels for Event Messages" on page 7.

To configure component logging to the system log server:

1. From configuration mode, access the configuration statement that configures the logging destination for the component. For example:

   ```
   [edit]
   user@host# component-hierarchy logger name syslog
   ```

   For example:

   ```
   [edit]
   user@host# edit shared sae configuration logger sae-sys-1 syslog
   ```

   ```
   [edit]
   user@host# edit snmp agent logger snmp-sys-1 syslog
   ```

   ```
   [edit]
   user@host# edit slot 0 jps logger jps-sys-1 syslog
   ```

2. (Optional) Specify the filter to define which event messages the software logs or disregards.

   ```
   [edit shared sae configuration logger sae-sys-1 syslog]
   user@host# set filter filter
   ```

Filters can specify the logging level, such as debug, or can specify expressions.

3. (Optional) Change the IP address or name of a host that collects event messages by means of a standard system logging daemon.

   [edit shared sae configuration logger sae-sys-1 syslog]
   user@host# set host *host*

   By default, the host is **loghost** for the system log server on the local host. (Configuration in the */etc/hosts* file sets **loghost** to **localhost**.)

   Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

4. (Optional) Specify the type of system log in accordance with the system logging protocol, a value of 0–23.

   [edit shared sae configuration logger sae-sys-1 syslog]
   user@host# set facility *facility*

5. (Optional) Specify the Message Format string that indicates how the information in an event message is printed.

   [edit shared sae configuration logger sae-sys-1 syslog]
   user@host# set format *format*

   Specify a Message Format string as defined in

   http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html

   The fields available for events are:

   - 0—Time and date of the event
   - 1—Name of the thread generating the event
   - 2—Text message of the event
   - 3—Category of the event
   - 4—Priority of the event

6. (Optional) Specify the port used for system logging, a value of 0–65535.

   [edit shared sae configuration logger sae-sys-1 syslog]
   user@host# set port *port*

Related Documentation

- Configuring an SRC Component to Store Log Messages in a File (SRC CLI) on page 27
- *Saving System Log Messages to a File (SRC CLI)*
- Configuration Statements for SRC Component Logging on page 41
- Before You Configure Logging for SRC Components on page 27
- Logging for SRC Components Overview on page 7

Configuring the Logrotate Utility (SRC CLI)

Use the options described in Table 10 on page 32 to configure global and local options for the logrotate utility. You set global options under the **[edit system logrotate logrotate.conf]** hierarchy level. You set local options for specific logging configuration files such as the **/var/log/wtmp** file under the **[edit system logrotate logrotate.conf logfiles *name*]** hierarchy level. You specify log rotation for system and SRC components under the **[edit system logrotate *file-name* logfiles]** hierarchy levels.

Table 10: Logrotate Options

Option	Description
compress	(Optional) Compress old versions of log files in gzip format.
delay-compress	(Optional) Postpone compression of the previous log file until the next rotation cycle. This option takes effect only when used in conjunction with the **compress** option. Use this option when a program cannot be instructed to close its log file and as a result may continue writing to the previous log file indefinitely.
copy	(Optional) Make a copy of the log file, but do not modify the original log file. Use this option to make a snapshot of the current log file, or when some other utility needs to truncate or parse the file. When you use this option, the create option has no effect because the original log file stays in place.
daily	(Optional) Rotate log files every day.
weekly	(Optional) Rotate log files weekly. This option rotates log files if the current weekday is earlier than the weekday of the last rotation or if more than a week has passed since the last rotation.
monthly	(Optional) Rotate log files monthly. This option rotates log files the first time that logrotate is run in a month (which is normally on the first day of the month).
rotate *rotate*	(Optional) Rotate log files the specified number times before removing them. If set to 0, old versions are removed rather than rotated.

Table 10: Logrotate Options *(continued)*

Option	Description
size *size*	(Optional) Rotate log files when they grow larger than the specified size in bytes. • If the size is followed by k, the size is assumed to be in kilobytes. • If the size is followed by M, the size is assumed to be in megabytes. • If the size is followed by G, the size is assumed to be in gigabytes. For example, **size 100**, **size 100k**, **size 100M**, or **size 100G** are all valid settings for this option. This option is mutually exclusive of the time interval options (daily, weekly, or monthly), and log files are rotated without regard for the last rotation time.
no-create	(Optional) Do not create new log files. This option overrides the settings under the **[edit system logrotate logrotate.conf create]**, **[edit system logrotate logrotate.conf logfiles** *name* **create]**, and **[edit system logrotate** *file-name* **logfiles** *name* **create]** hierarchy levels.
copy-truncate	(Optional) When set, this option copies the active log file to a backup and truncates the active log file. Truncate the original log file in place after creating a copy, instead of moving the old log file and optionally creating a new one. This option is useful when programs cannot be instructed to close their log file and as a result, may continue writing (appending) to the previous log file indefinitely. NOTE: There is a very small time period between copying the file and truncating it, so some logging data might be lost. When you specify this option, the create option has no effect because the old log file stays in place.
if-empty	(Optional) Rotate the log file even if it is empty.
missing-ok	(Optional) If the log file is missing, go on to the next log file without issuing an error message.
filenames *filenames*	(Optional) Names of the log files to rotate. Separate filenames with a space.

Table 10: Logrotate Options *(continued)*

Option	Description
shared-scripts	(Optional) Normally, the scripts you specify with the **pre-rotate** and **post-rotate** options are run for each log that is rotated and the absolute path to the log file is passed as the first argument to the script. This means a single script may be run multiple times for log file entries that match multiple files. If you specify the **shared-scripts** option, the scripts are run only once, regardless of how many logs match the wildcard pattern, and the entire pattern is passed to them. However, if none of the logs in the pattern require rotating, the scripts are not run at all. If the scripts exit with an error, the remaining actions are not executed for any log.
pre-rotate *pre-rotate*	(Optional) The lines between the pre-rotate and endscript (both of which must appear on lines by themselves) are executed (using /bin/sh) before the log file is rotated and only if the log is actually to be rotated. These directives may appear only inside a log file definition. Normally, the absolute path to the log file is passed as the first argument to the script. If the **shared-scripts** option is specified, the whole pattern is passed to the script.
post-rotate *post-rotate*	(Optional) The lines between the post-rotate and endscript (both of which must appear on lines by themselves) are executed (using /bin/sh) after the log file is rotated. These directives may appear only inside a log file definition. Normally, the absolute path to the log file is passed as the first argument to the script. If the **shared-scripts** option is specified, the entire pattern is passed to the script.
first-action *first-action*	(Optional) The lines between first-action and endscript (both of which must appear on lines by themselves) are executed (using /bin/sh) once before all log files that match the wildcard pattern are rotated, before the pre-rotate script is run, and only if at least one log is to be rotated. These directives may appear only inside a log file definition. The entire pattern is passed to the script as the first argument. If the script exits with an error, no further processing is performed.
last-action *last-action*	(Optional) The lines between last-action and endscript (both of which must appear on lines by themselves) are executed (using /bin/sh) once after all log files that match the wildcard pattern are rotated, after the post-rotate script is run, and only if at least one log is rotated. These directives may appear only inside a log file definition. The entire pattern is passed to the script as the first argument. If the script exits with an error, only an error message is shown (because this is the last action).

Use the options described in Table 11 on page 35 under the **[edit system logrotate logrotate.conf create]**, **[edit system logrotate logrotate.conf logfiles *name* create]**, and **[edit system logrotate *file-name* logfiles *name* create]** hierarchy levels to specify the permissions, owner, and group of new log files. The default is to use the same mode, owner, and group as the original file.

Table 11: Options for Specifying How Log Files are Created

Option	Description
default	Create new log files with the same mode, owner, and group as the original file.
mode *mode*	Create new log files with the specified mode in octal format.
owner *owner*	Create new log files with the specified owner (username).
group *group*	Create new log files with the specified group.

- Configuring the Global Options for the Logrotate Utility on page 35
- Configuring Log Rotation Options for Specific Logging Configuration Files on page 35
- Configuring Logging Rotation Options for System and SRC Components (SRC CLI) on page 36

Configuring the Global Options for the Logrotate Utility

To configure global options for the logrotate utility:

NOTE: **The CLI editing level must be set to expert to set the global options.**

1. From configuration mode, access the configuration statement that configures global options for the logrotate utility.

   ```
   [edit]
   user@host# edit system logrotate logrotate.conf
   ```

2. Specify how you want to rotate and compress the log files by setting the desired options listed in Table 10 on page 32. For example, to rotate log files weekly and compress them:

   ```
   [edit system logrotate logrotate.conf]
   user@host# set weekly
   user@host# set compress
   ```

3. Specify how you want to create new log files by setting the options listed in Table 11 on page 35. For example, to use the default setting:

   ```
   [edit system logrotate logrotate.conf]
   user@host# edit create
   user@host# set default
   ```

Configuring Log Rotation Options for Specific Logging Configuration Files

Use the following procedure to configure log rotation options for specific files such as the **/var/log/wtmp** file.

To configure local options for the logrotate utility:

1. From configuration mode, access the configuration statement that configures local options for the logrotate utility and specify one or more log filenames. Separate log filenames with a space.

   ```
   [edit]
   user@host# edit system logrotate logrotate.conf logfiles name
   ```

2. Specify how you want to rotate and compress the log files by setting the desired options listed in Table 10 on page 32. For example, to rotate log files weekly:

   ```
   [edit system logrotate logrotate.conf logfiles name]
   user@host# set weekly
   ```

3. Specify how you want to create new log files by setting the options listed in Table 11 on page 35. For example, to use the default setting:

   ```
   [edit system logrotate logrotate.conf logfiles name]
   user@host# edit create
   user@host# set default
   ```

Configuring Logging Rotation Options for System and SRC Components (SRC CLI)

Options you configure for system and specific SRC components override global and local options of the same name.

To configure log rotation options for the system or for SRC components:

1. From configuration mode, access the configuration statement to configure local options and specify the filename used by the SRC component.

   ```
   [edit]
   user@host# edit system logrotate file-name
   ```

   For example, to specify local options for the ACP component:

   ```
   [edit]
   user@host# edit system logrotate UMCacp
   ```

2. Specify the name of one or more log files for which you want to configure compression and rotation options. Separate log filenames with a space.

   ```
   [edit system logrotate UMCacp]
   user@host# edit logfiles name
   ```

   For example, to specify the UMCacp-1 log file:

   ```
   [edit system logrotate UMCacp]
   user@host# edit logfiles UMCacp-1
   ```

3. Specify how you want to rotate and compress the log files by setting the desired options listed in Table 10 on page 32. For example, to rotate log files weekly:

```
[edit system logrotate UMCacp logfiles UMCacp-1]
user@host# set weekly
```

4. Specify how you want to create new log files by setting the options listed in Table 11 on page 35. For example, to use the default setting:

```
[edit system logrotate UMCacp logfiles UMCacp-1]
user@host# edit create
user@host# set default
```

Related Documentation

- Logging for SRC Components Overview on page 7
- Rotating Log Files on page 22
- Configuration Statements for the Logrotate Utility (SRC CLI) on page 42

Configuring ACP to Store Log Messages in a File (C-Web Interface)

To configure component logging for ACP:

1. Click **Configure**, expand **Shared**, expand **ACP**, and then click **Configuration**.

   The Configuration pane appears.
2. From the Create new list, select **Logger**.
3. In the dialog box, type a name for the new logger, and click **OK**.

   The name of the logger appears in the side pane and the Logger pane.
4. Expand the logger in the side pane, and then click **File** or **Syslog**.
5. Click **Create,** enter information as described in the Help text in the main pane, and click **Apply**.

Related Documentation

- Configuring an SRC Component to Store Log Messages in a File (SRC CLI) on page 27
- Configuring the SAE to Store Log Messages in a File (C-Web Interface) on page 37
- Configuring NIC to Store Log Messages in a File (C-Web Interface) on page 38
- *Configuring SRC ACP (C-Web Interface)*
- *SRC ACP Overview*

Configuring the SAE to Store Log Messages in a File (C-Web Interface)

To configure component logging for SAE:

1. Click **Configure**, expand **Shared**, expand **ACP**, and then click **Configuration**.

   The Configuration pane appears.
2. From the Create new list, select **Logger**.

The name of the logger appears in the side pane and the Logger pane.

3. Expand the logger in the side pane, and then click **File** or **Syslog**.
4. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Related Documentation

- Configuring an SRC Component to Store Log Messages in a File (SRC CLI) on page 27
- Configuring ACP to Store Log Messages in a File (C-Web Interface) on page 37
- Configuring NIC to Store Log Messages in a File (C-Web Interface) on page 38
- Configuring the SNMP to Store Log Messages in a File (C-Web Interface) on page 38
- Configuring JPS to Store Log Messages in a File (C-Web Interface) on page 39

Configuring NIC to Store Log Messages in a File (C-Web Interface)

To configure component logging for NIC:

1. Click **Configure**, expand **Shared**, and then click **NIC**.

   The NIC pane appears.
2. In the side pane, expand a configuration scenario, such as Scenario:OnePopSharedlp.
3. In the side pane, expand a host, such as Demohost.

   The Hosts pane appears.
4. From the Create new list, select **Logger**.

   The name of the logger appears in the side pane and the Logger pane.
5. Expand the logger in the side pane, and then click **File** or **Syslog**.
6. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Related Documentation

- Configuring an SRC Component to Store Log Messages in a File (SRC CLI) on page 27
- Configuring ACP to Store Log Messages in a File (C-Web Interface) on page 37
- Configuring the SAE to Store Log Messages in a File (C-Web Interface) on page 37
- Configuring the SNMP to Store Log Messages in a File (C-Web Interface) on page 38
- Configuring JPS to Store Log Messages in a File (C-Web Interface) on page 39

Configuring the SNMP to Store Log Messages in a File (C-Web Interface)

To configure component logging for SNMP:

1. Click **Configure**, expand **Snmp**, and then click **Agent**.

   The Agent pane appears.

2. From the Create new list, select **Logger**.

   The name of the logger appears in the side pane and the Logger pane.

3. Expand the logger in the side pane, and then click **File** or **Syslog**.

4. Click **Create,** enter information as described in the Help text in the main pane, and click **Apply**.

Related Documentation

- Configuring an SRC Component to Store Log Messages in a File (SRC CLI) on page 27
- Configuring ACP to Store Log Messages in a File (C-Web Interface) on page 37
- Configuring the SAE to Store Log Messages in a File (C-Web Interface) on page 37
- Configuring NIC to Store Log Messages in a File (C-Web Interface) on page 38
- Configuring JPS to Store Log Messages in a File (C-Web Interface) on page 39

Configuring JPS to Store Log Messages in a File (C-Web Interface)

To configure component logging for JPS:

1. Click **Configure**, expand **Slot**, and then expand the slot for which you want to configure component logging.

2. Click **JPS**.

   The JPS pane appears.

3. From the Create new list, select **Logger**.

   The name of the logger appears in the side pane and the Logger pane.

4. Expand the logger in the side pane, and then click **File** or **Syslog**.

5. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Related Documentation

- Configuring an SRC Component to Store Log Messages in a File (SRC CLI) on page 27
- Configuring ACP to Store Log Messages in a File (C-Web Interface) on page 37
- Configuring the SAE to Store Log Messages in a File (C-Web Interface) on page 37
- Configuring NIC to Store Log Messages in a File (C-Web Interface) on page 38
- Configuring the SNMP to Store Log Messages in a File (C-Web Interface) on page 38

CHAPTER 4

Configuration Statements

Configuration Statements for SRC Component Logging

Use the following configuration statements to configure logging for SRC components. You access these statements from the hierarchy for a component, such as:

- **[edit shared acp configuration]**
- **[edit shared sae configuration]**
- **[edit shared nic scenario** *scenario-name* **]**
- **[edit snmp agent]**
- **[edit slot 0 jps]**

```
logger name {
    file-logger {
        device-filter-key device-filter-key;
        filter filter ;
        filename filename ;
        rollover-filename rollover-filename ;
        maximum-file-size maximum-file-size ;
    }
    syslog-logger {
        filter filter ;
        port port ;
        syslog-host syslog-host ;
        syslog-facility syslog-facility ;
        format  format ;
    }
}
```

NOTE: The **device-filter-key** option is available only on the SAE component.

For detailed information about each configuration statement, see *SRC PE CLI Command Reference*.

Related Documentation

- Configuring System Logging (SRC CLI) on page 30
- Configuring an SRC Component to Store Log Messages in a File (SRC CLI) on page 27
- Before You Configure Logging for SRC Components on page 27
- Logging for SRC Components Overview on page 7
- Categories and Severity Levels for Event Messages on page 7

Configuration Statements for the Logrotate Utility (SRC CLI)

Use the following statements to configure the logrotate utility:

```
system logrotate file-name{
}
system logrotate file-name logfiles name {
    compress;
    delay-compress;
    copy;
    daily;
    weekly;
    monthly;
    rotate rotate;
    size size;
    no-create;
    copy-truncate;
    if-empty;
    missing-ok;
    filenames filenames;
    shared-scripts;
    pre-rotate pre-rotate;
    post-rotate post-rotate;
    first-action first-action;
    last-action last-action;
}
system logrotate file-name logfiles name create {
    default;
    mode mode;
    owner owner;
    group group;
}
system logrotate logrotate.conf {
    compress;
    delay-compress;
    copy;
    daily;
    weekly;
    monthly;
    rotate rotate;
    size size;
    no-create;
    copy-truncate;
    if-empty;
    missing-ok;
```

```
}
system logrotate logrotate.conf create {
    default;
    mode mode;
    owner owner;
    group group;
}
system logrotate logrotate.conf logfiles name {
    compress;
    delay-compress;
    copy;
    daily;
    weekly;
    monthly;
    rotate rotate;
    size size;
    no-create;
    copy-truncate;
    if-empty;
    missing-ok;
    filenames filenames;
    shared-scripts;
    pre-rotate pre-rotate;
    post-rotate post-rotate;
    first-action first-action;
    last-action last-action;
}
system logrotate logrotate.conf logfiles name create {
    default;
    mode mode;
    owner owner;
    group group;
}
```

Related Documentation

- Logging for SRC Components Overview on page 7
- Rotating Log Files on page 22
- Configuring the Logrotate Utility (SRC CLI) on page 32

PART 3

Administration

CHAPTER 5

Routine Monitoring

Viewing Information About Components Installed (SRC CLI)

Purpose View release and status information for SRC components installed on a system.

Action

```
user@host> show component

Installed Components
Name    Version                  Status
cli       Release: 7.0 Build: CLI.A.7.0.0.0171              running
acp       Release: 7.0 Build: ACP.A.7.0.0.0174              disabled
jdb       Release: 7.0 Build: DIRXA.A.7.0.0.0176            running
editor    Release: 7.0 Build: EDITOR.A.7.0.0.0176           running
redir     Release: 7.0 Build: REDIR.A.7.0.0.0176            disabled
licSvr    Release: 7.0 Build: LICSVR.A.7.0.0.0179           stopped
nic       Release: 7.0 Build: GATEWAY.A.7.0.0.0170          disabled
sae       Release: 7.0 Build: SAE.A.7.0.0.0166              running
www       Release: 7.0 Build: UMC.A.7.0.0.0169              disabled
jps       Release: 7.0 Build: JPS.A.7.0.0.0172              disabled
agent     Release: 7.0 Build: SYSMAN.A.7.0.0.0174           running
webadm    Release: 7.0 Build: WEBADM.A.7.0.0.0173           disabled
```

Meaning Table 12 on page 47 describes the output fields for the **show component** command. Output fields are listed in the order in which they appear.

Table 12: Output Fields for show component

Field Name	Field Description
Name	Name of the component
Version	Version of the component
Status	State of the component, running or disabled

Related Documentation

- Viewing Information About Components Installed (C-Web Interface) on page 48
- *Viewing C Series Controller Information*

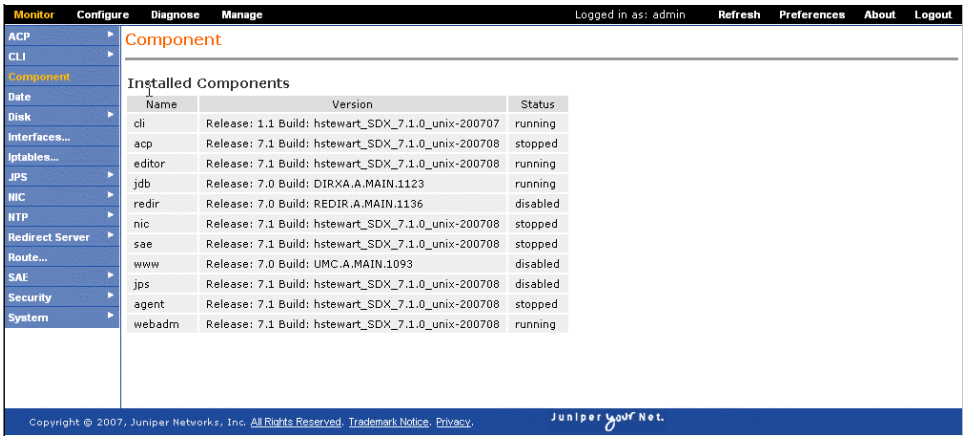
- *Directories on the C Series Controller*

Viewing Information About Components Installed (C-Web Interface)

Purpose View the installed SRC components.

Action Click **Monitor**>**Component**.

The Component pane displays the status of each installed component.



Related Documentation

- Viewing Information About Components Installed (SRC CLI) on page 47
- *Viewing C Series Controller Information*
- *Directories on the C Series Controller*

CHAPTER 6

Monitoring Commands

SRC Monitoring Options

Table 13 on page 49 lists and compares the monitoring options for the C-Web interface and the SRC CLI.

Table 13: Comparison of SRC Monitoring Options

C-Web Interface Monitor Option	Information Displayed	Corresponding SRC CLI Commands
ACP	Admission Control Plug-In (ACP) data and statistics	• show acp backbone congestion-point congestion-point-expression • show acp backbone congestion-point dn • show acp backbone service • show acp edge congestion-point dn • show acp edge congestion-point subscriber-session-id • show acp edge subscriber • show acp remote-update congestion-point dn • show acp remote-update congestion-point name • show acp remote-update subscriber • show acp statistics device • show acp statistics directory • show acp statistics general
CLI	SRC CLI level and authorization data	• show cli • show cli authorization
Component	Installed components	• show component
Date	System date and time	• show date
Disk	System disk status	• show disk status

Table 13: Comparison of SRC Monitoring Options *(continued)*

C-Web Interface Monitor Option	Information Displayed	Corresponding SRC CLI Commands
Interfaces	System interfaces	• show interfaces
Iptables	Filtered traffic statistics from the iptables Linux tool	• show iptables
JPS	Juniper Policy Server (JPS) data and statistics	• show jps statistics • show jps statistics am • show jps statistics am connections • show jps statistics cmts-locator • show jps statistics cmts • show jps statistics_cmts connections • show jps statistics message-handler • show jps statistics message-handler message-flow • show jps statistics process • show jps statistics rks
NIC	Network information collector (NIC) component configuration data and statistics, including NIC agents, resolvers, and process	• show nic data • show nic data agent • show nic data resolver • show nic statistics • show nic statistics agent • show nic statistics host • show nic statistics process • show nic statistics resolver • show nic slot number data • show nic slot number statistics
NTP	Network Time Protocol (NTP) configuration data and statistics	• show ntp associations • show ntp statistics • show ntp status
Redirect server	Redirect server statistics	• show redirect server statistics
Route	Route data from the local system to a remote host	• show route

Table 13: Comparison of SRC Monitoring Options *(continued)*

C-Web Interface Monitor Option	Information Displayed	Corresponding SRC CLI Commands
SAE	SAE configuration data and statistics	• show sae drivers • show sae interfaces • show sae licenses • show sae policies • show sae registered equipment • show sae registered login • show sae services • show sae statistics device • show sae statistics device common • show sae statistics directory • show sae statistics directory connections • show sae statistics license client • show sae statistics license device • show sae statistics license local • show sae statistics policy-management • show sae statistics process • show sae statistics radius • show sae statistics radius client • show sae statistics sessions • show sae subscribers • show sae subscribers accounting-user-id • show sae subscribers dn • show sae subscribers ip • show sae subscribers login-name • show sae subscribers service-name • show sae subscribers session-id • show sae threads
Security	Security certificate configuration and statistics	• show security certificate
System	SRC software and C Series Controller configuration data	• show configuration • show system boot-messages • show system information • show system ldap community • show system ldap server • show system ldap statistics • show system users

Related Documentation

- *Monitoring and Troubleshooting Tools Overview*
- *Monitoring with the SRC CLI and the C-Web Interface*

PART 4

Index

Index